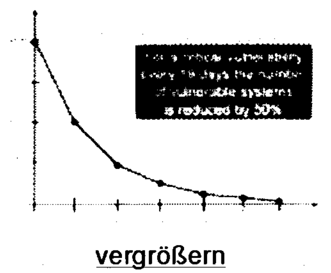
21.11.2005 15:00 Uhr

Unternehmen sind nicht sicher vor Attacken

# Immer neue Lücken im Firmen-System

Fast 70 Prozent der Geschäftssysteme sind immer noch nicht vor Angriffen geschützt. Obwohl zurzeit viel Unternehmen ihre gesamten Systeme umstellen sind sie nicht sicher, so die Analyse "Gesetze der Schwachstellen" des Lösungsanbieters Qualys.



Unternehmen haben ihre Patching-Prozesse verbessert und können dadurch schneller Schwachstellen beseitigen.

vergrößern

Die häufigsten und kritischsten Sicherheitslücken konnten geschlossen werden. Die Ergebnisse zeigen, dass Unternehmen ihre Patching-Prozesse verbessert haben. Laut der Untersuchung benötigen Firmen durchschnittlich 19 Tage, um die Hälfte ihrer gefährdeten Internetsysteme auszubessern. Im vergangenen Jahr waren es 21 und vor zwei Jahren noch 30 Tage.

**"2005 war das Jahr der Verbesserungen beim Patching und Aktualisieren** anfälliger Systeme", sagt Gerhard Eschelbeck, CTO und VP Engineering bei Qualys. Viele Software-Anbieter gäben jetzt regelmäßig Advisories mit Patch-Updates heraus. Das führe dazu, dass sich Unternehmen schneller um Korrekturen bemühen als bei ungeregelten Abläufen.

Laut der Analyse verkürzt sich die Zeit von der Bekanntgabe einer Schwachstelle bis zu deren Entdeckung (Time to Exploit) bei automatisierten Angriffen weiterhin dramatisch. Sie richten zurzeit 85 Prozent ihres Schadens innerhalb der ersten 15 Tage an.

Der Untersuchung zufolge ist die Bedrohung für drahtlose Systeme sehr gering. Nur eine von etwa 20.000 kritischen Sicherheitslücken betraf ein Wireless-Gerät. Allerdings verlagern sich die Schwachstellen von der Server- auf die zu Client-Seite. Mehr als 60 Prozent aller neuen kritischen Sicherheitslücken finden sich in Kunden-Anwendungen. So tappen Anwender in Software-Schwachstellen, indem sie beispielsweise eine bösartige Website aufsuchen oder einen infizierten Mail-Anhang öffnen.

Im Wesentlichen hat die Studie sechs Ergebnisse hervorgebracht:

**1. Halbwertzeit**

Im vergangenen Jahr verkürzte sich die Halbwertzeit kritischer Schwachstellen in externen Systemen von 21 auf 19 Tage und in internen Systemen von 62 auf 48 Tage. Wenn neue Sicherheitslücken regelmäßig, nach einem vorgegebenen Zeitplan bekannt gemacht werden, installieren Unternehmen die entsprechenden Patches um 18 Prozent schneller. Die Halbwertzeit beschreibt, wie lange Anwender brauchen, um die Hälfte ihrer Systeme durch Patches zu schützen und so die Gefährdung zu verkleinern

**2. Verbreitung**

Jedes Jahr werden 50 Prozent der am meisten verbreiteten und kritischen Schwachstellen durch neue Sicherheitslücken abgelöst.

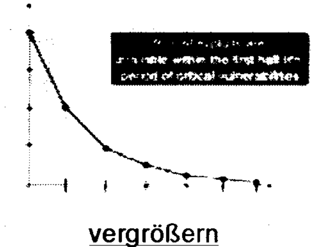
**3. Wirkungsdauer**

Vier Prozent aller kritischen Schwachstellen bleiben bestehen und haben eine unbegrenzte Lebensdauer.

**4. Fokus**

90 Prozent aller Gefährdungen durch Sicherheitslücken gehen von zehn Prozent der kritischen Schwachstellen aus.

## 5. Fenster der Gefährdung



vergrößern

80 Prozent aller Exploits werden innerhalb der ersten Halbwertzeit entwickelt.

Der Time-to-Exploit-Zyklus schrumpft schneller als der Zyklus der Schwachstellenbeseitigung. 80 Prozent aller Exploits werden innerhalb der ersten Halbwertszeit kritischer Schwachstellen entwickelt.

## 6. Ausnutzung

Automatisierte Angriffe richten 85 Prozent des von ihnen verursachten Schadens innerhalb der ersten 15 Tage nach ihrem Ausbruch an und haben eine unbegrenzte Lebenszeit.

Die Ergebnisse basieren auf der statistischen Analyse von fast 21 Millionen kritischen Schwachstellen, die bei 32 Millionen Live-Netzwerk-Scans entdeckt wurden.